AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for encrypting data, the method comprising:

providing a first data processing system;

providing a second data processing system including program instructions to generate a session key, to encrypt ~~decrypt~~ original data using the session key, to encrypt the session key with a first user's public key, to encrypt the session key with a master public key, to generate a first data packet including a plurality of encrypted session keys and encrypted data, and to transmit the first data packet to the first data processing system;

generating and transmitting a second data packet including the encrypted session keys and the encrypted data to another data processing system instead of or in addition to the first data processing system; and ~~the data packet to another data processing system instead of or in addition to the first data processing system using the first user's public key, the session key, a new session key and the master public key;~~ ~~and~~

the first data processing system receiving the first data packet and including program instructions to decrypt one of the encrypted session keys with a private key of the first user, and to decrypt the encrypted data with the session key to re-create the original data.

2. (Cancelled).

3. (Cancelled).

4. (Cancelled).

5. (Cancelled).

6. (Cancelled).

7. (Previously Presented) The method, as set forth in claim 1, further comprising storing the user's private key on a data storage medium coupled to the destination data processing system.

8. (Previously Presented) The method, as set forth in claim 1, further comprising storing the master private key on a data storage medium coupled to the destination data processing system.

9. (Previously Presented) The method, as set forth in claim 7, further comprising retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

10. (Previously Presented) The method, as set forth in claim 1, further comprising retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

11. (Original) The method, as set forth in claim 1, further comprising utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

12. (Currently Amended) A method for encrypting data comprising:

providing a first data processing system;

providing a second data processing system including program instructions to generate a session key, to encrypt ~~decrypt~~ original data using the session key, to encrypt the session key with a first user's public key, to encrypt the session key with a master public key, to generate a first data packet including a plurality of encrypted session keys and encrypted data, and to transmit the first data packet to the first data processing system;

generating and transmitting a second data packet including the encrypted session keys and the encrypted data to another data processing system instead of or in addition to the first data processing system; ~~the data packet to another data processing system instead of or in addition to the first data processing system using the first user's public key, the session key, a new session key and the master public key;~~

the first data processing system receiving the first data packet and including program instructions to decrypt one of the encrypted session keys with a private key of the first user, and to decrypt the encrypted data with the session key to re-create the original data; and

the master public key and a master private key allowing another user to gain access to encrypted data, the other user executing program instructions on the first data processing system to decrypt the one encrypted session key using the master private key, and to decrypt the encrypted data with the session key to re-create the original data.

13. (Cancelled).

14. (Cancelled).

15. (Cancelled).

16. (Cancelled).

17. (Cancelled).

18. (Previously Presented) The method as set forth in claim 12, wherein the user's private key is stored on a data storage medium coupled to the second data processing system.

19. (Previously Presented) The method as set forth in claim 12, wherein the master private key is stored on a data storage medium coupled to the second data processing system.

20. (Previously Presented) The method as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the user's private key from a smart card.

21. (Previously Presented) The method as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the master private key from a smart card.

22. (Previously Presented) The method as set forth in claim 12, further comprising:
a plurality of master private keys; and
a plurality of master public keys.

23. (Cancelled).

24. (Cancelled).

25. (Cancelled).

26. (Cancelled).

27. (Cancelled).

28. (Cancelled).

29. (Cancelled).